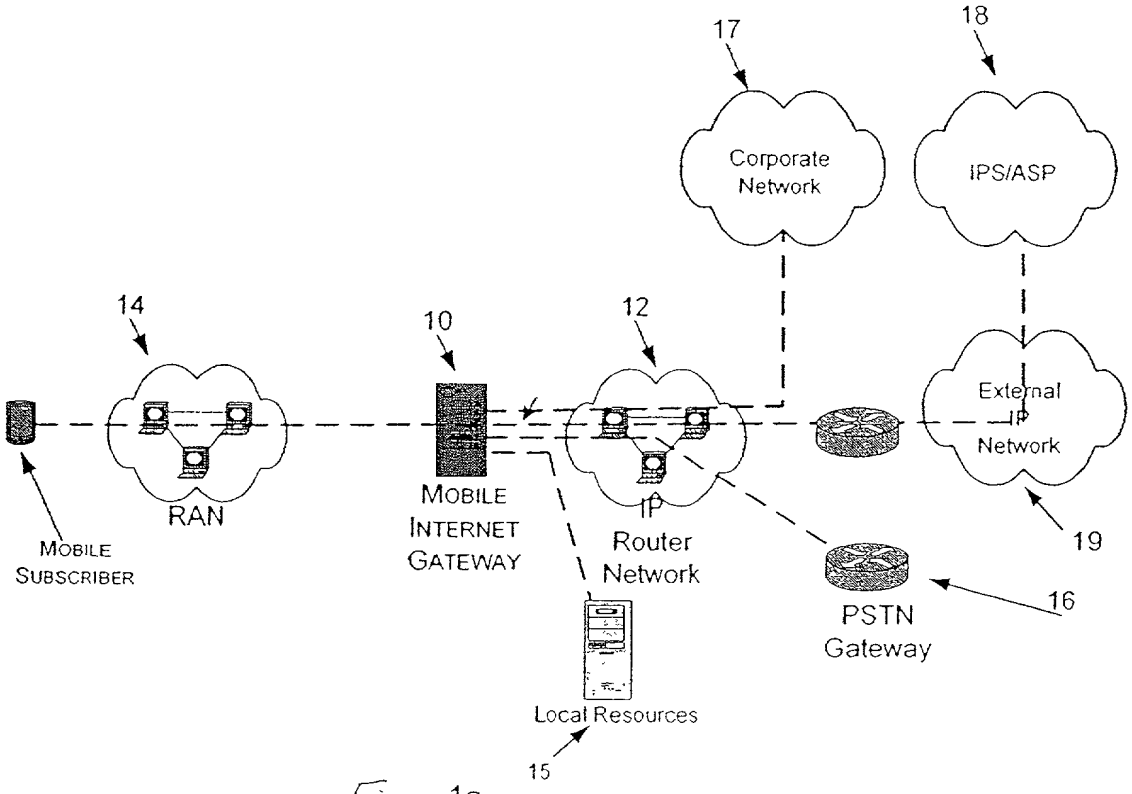
17
18
Corporate Network
IPS/ASP
14
10
12
External IP Network
MOBILE SUBSCRIBER
RAN
MOBILE INTERNET GATEWAY
IP Router Network
19
16
PSTN Gateway
Local Resources
15

Fig. 1a

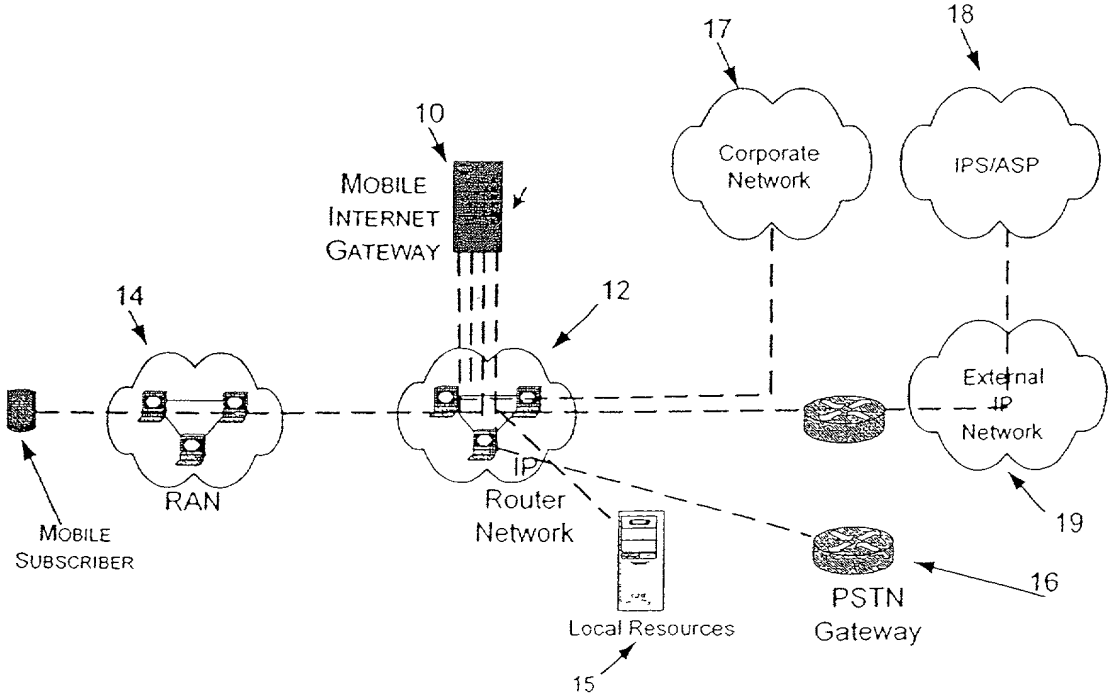
17
18
10
Corporate Network
IPS/ASP
MOBILE INTERNET GATEWAY
14
12
External IP Network
RAN
IP Router Network
19
MOBILE SUBSCRIBER
16
PSTN Gateway
Local Resources
15

Fig. 1b

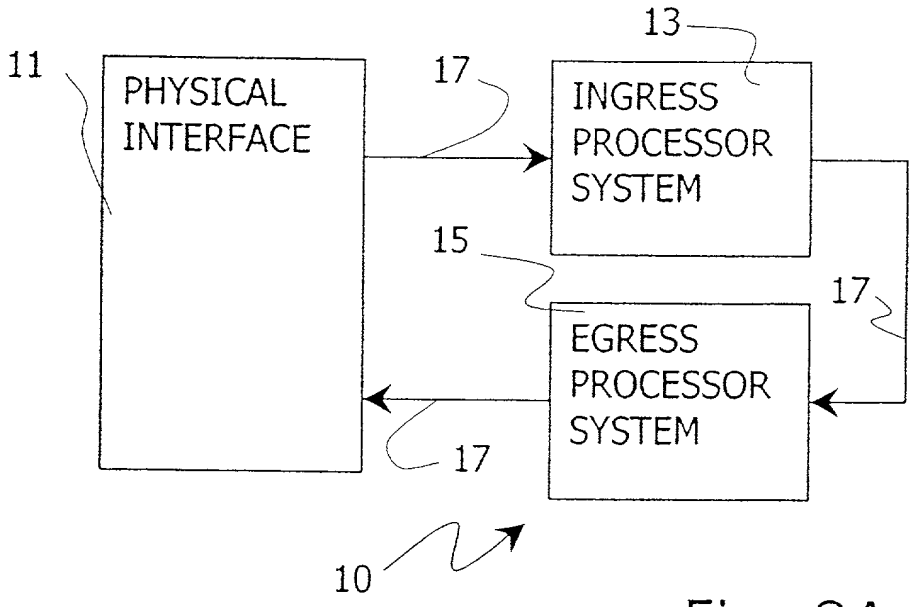
11
PHYSICAL INTERFACE
17
13
INGRESS PROCESSOR SYSTEM
15
17
EGRESS PROCESSOR SYSTEM
17
10

Fig. 2A

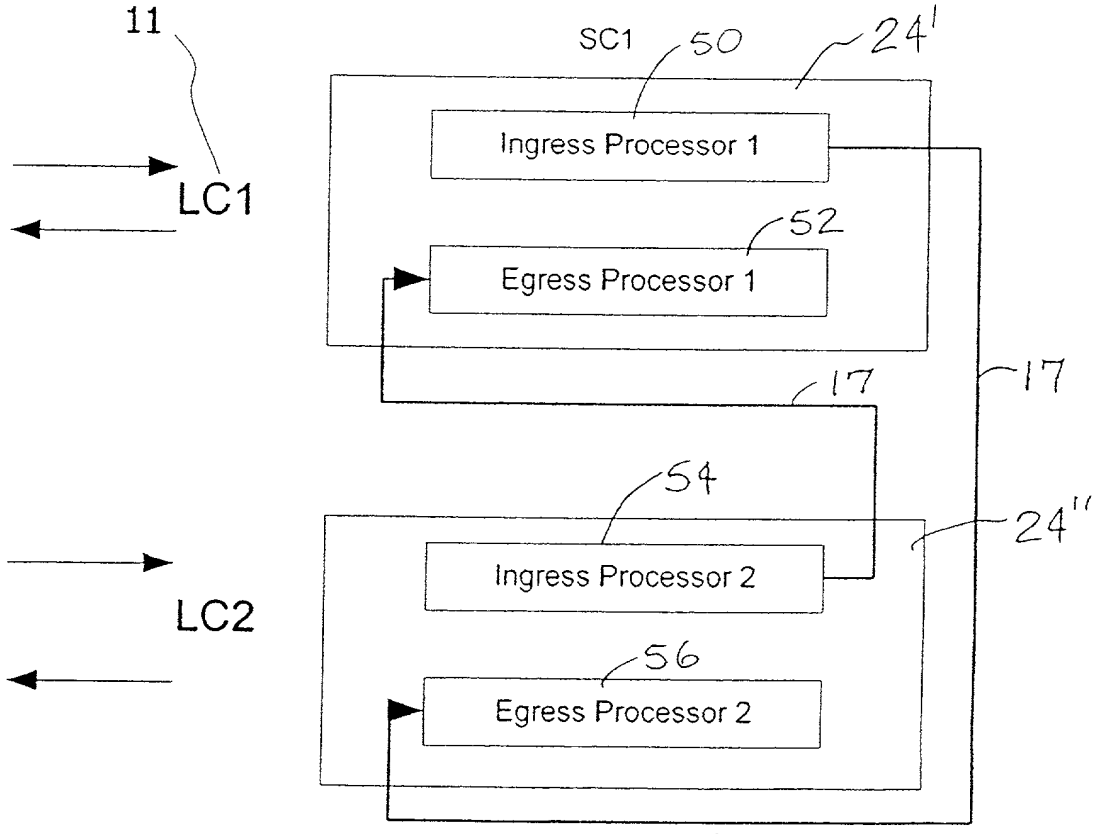
11
LC1
SC1
50
24'
Ingress Processor 1
52
Egress Processor 1
17
17
54
24''
Ingress Processor 2
LC2
56
Egress Processor 2

Fig. 2B

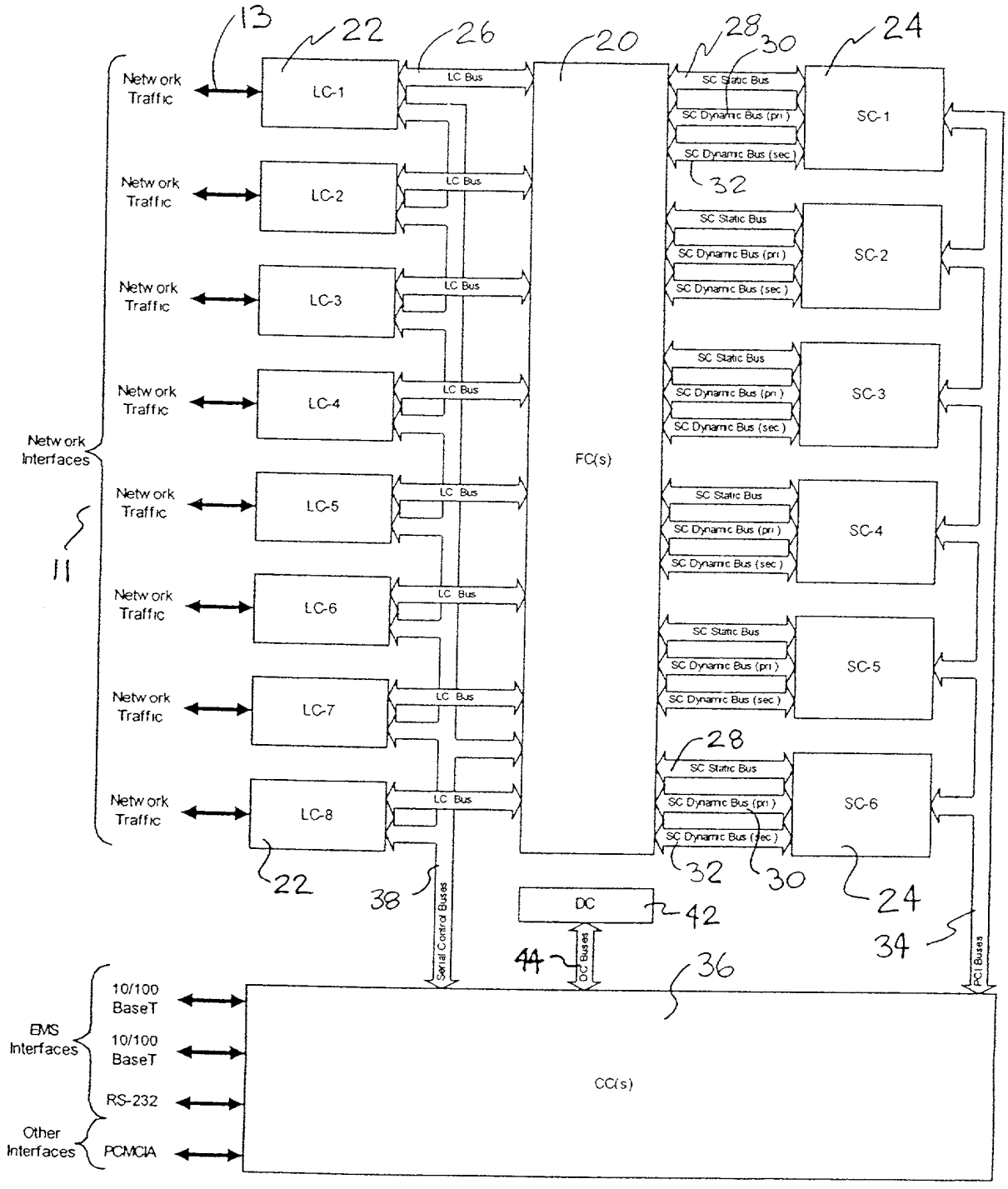
13
22
26
20
28
30
24
Network Traffic
LC-1
LC Bus
SC Static Bus
SC Dynamic Bus (pri)
SC Dynamic Bus (sec)
SC-1
32
LC-2
SC-2
LC-3
SC-3
LC-4
Network Interfaces
FC(s)
LC-5
SC-4
11
LC-6
SC-5
LC-7
LC-8
22
38
Serial Control Busses
DC
42
44
I2C Busses
34
PCI Busses
36
10/100 BaseT
EMS Interfaces
RS-232
Other Interfaces
PCMCIA
CC(s)

Fig. 3

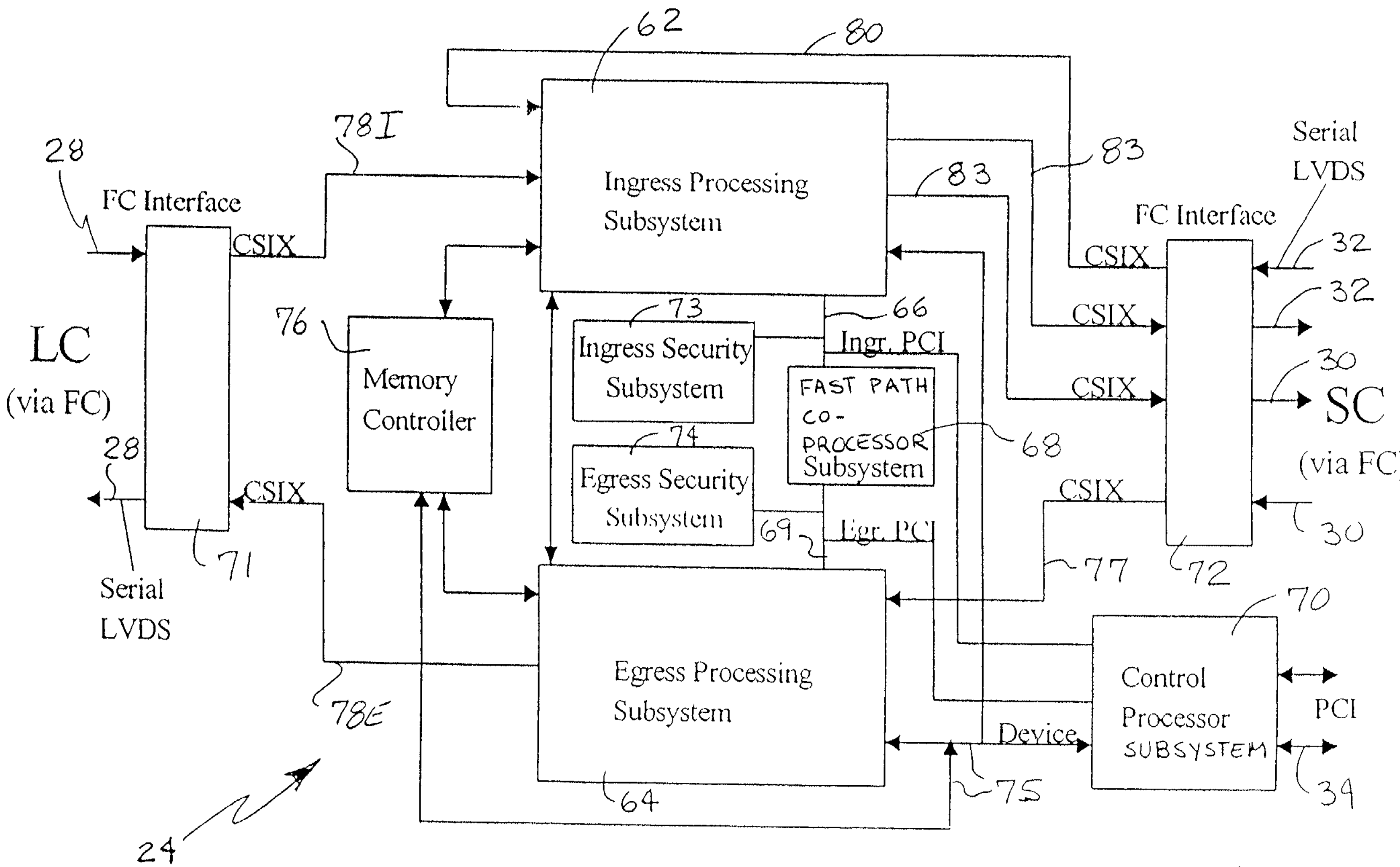
62
80
28
FC Interface
CSIX
78I
Ingress Processing
Subsystem
83
83
Serial
LVDS
FC Interface
CSIX
32
CSIX
32
CSIX
30
SC
(via FC)
LC
(via FC)
76
Memory
Controller
73
Ingress Security
Subsystem
66
Ingr. PCI
FAST PATH
CO-
PROCESSOR
Subsystem
68
28
CSIX
74
Egress Security
Subsystem
69
Egr. PCI
CSIX
30
71
72
77
Serial
LVDS
70
Egress Processing
Subsystem
Control
Processor
SUBSYSTEM
PCI
78E
Device
34
75
64
24

Fig. 4

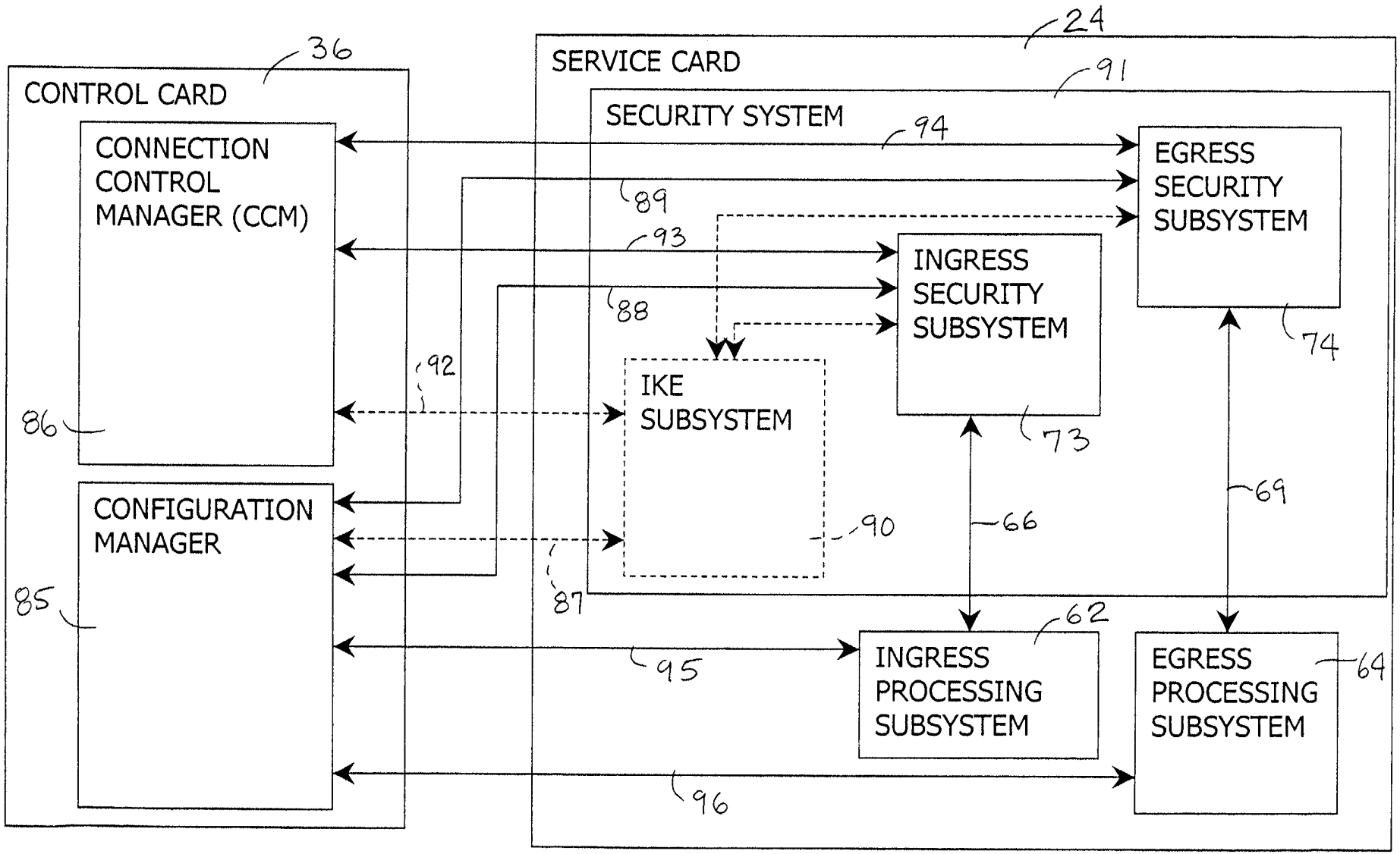
24
SERVICE CARD
91
SECURITY SYSTEM
36
CONTROL CARD
CONNECTION CONTROL MANAGER (CCM)
86
CONFIGURATION MANAGER
85
94
89
93
88
92
IKE SUBSYSTEM
90
87
EGRESS SECURITY SUBSYSTEM
74
INGRESS SECURITY SUBSYSTEM
73
66
69
62
INGRESS PROCESSING SUBSYSTEM
EGRESS PROCESSING SUBSYSTEM
64
95
96

Fig. 5

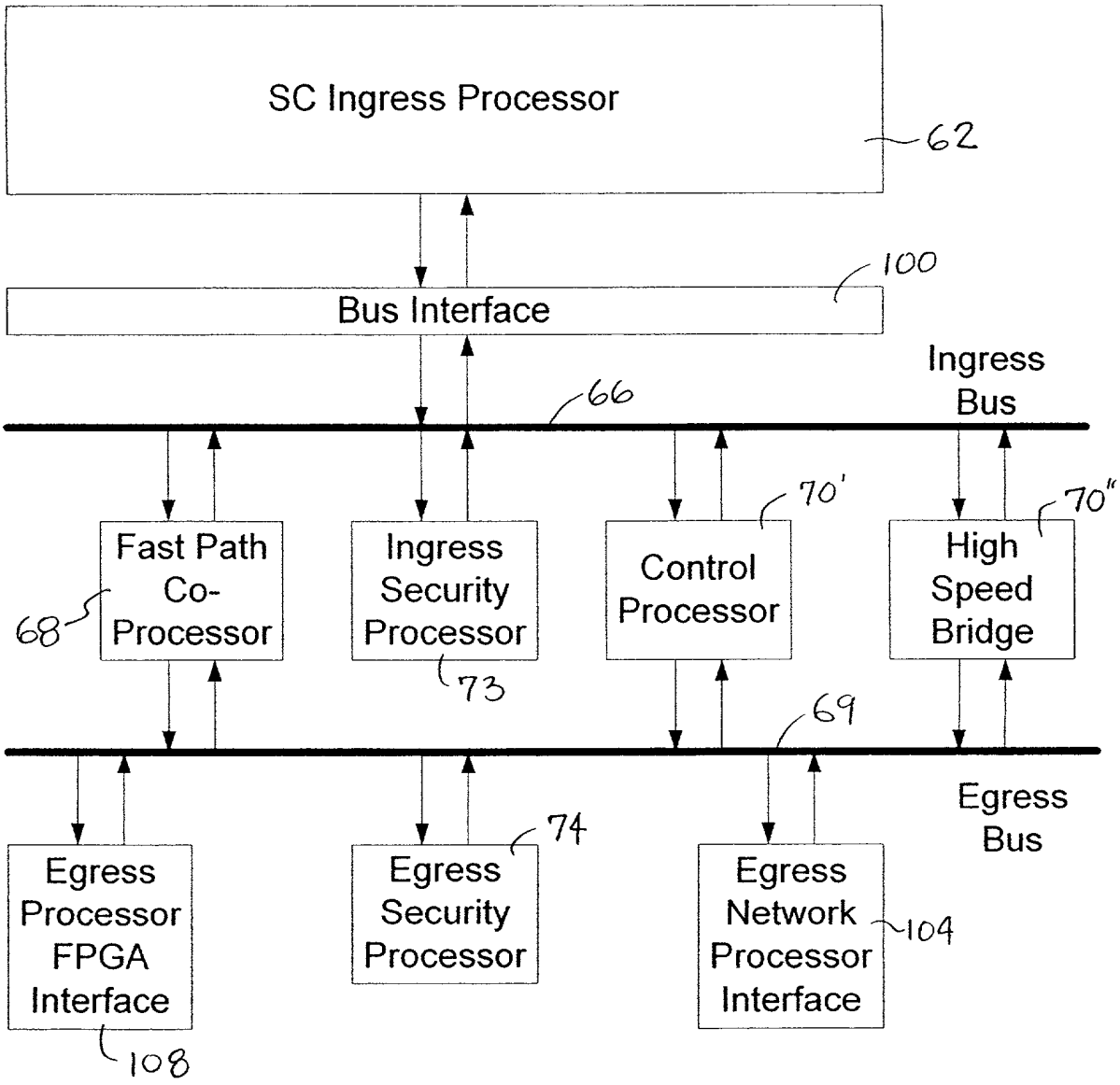
SC Ingress Processor
62
Bus Interface
100
Ingress Bus
66
Fast Path Co-Processor
68
Ingress Security Processor
73
Control Processor
70'
High Speed Bridge
70"
69
Egress Bus
Egress Processor FPGA Interface
108
Egress Security Processor
74
Egress Network Processor Interface
104

Fig. 6

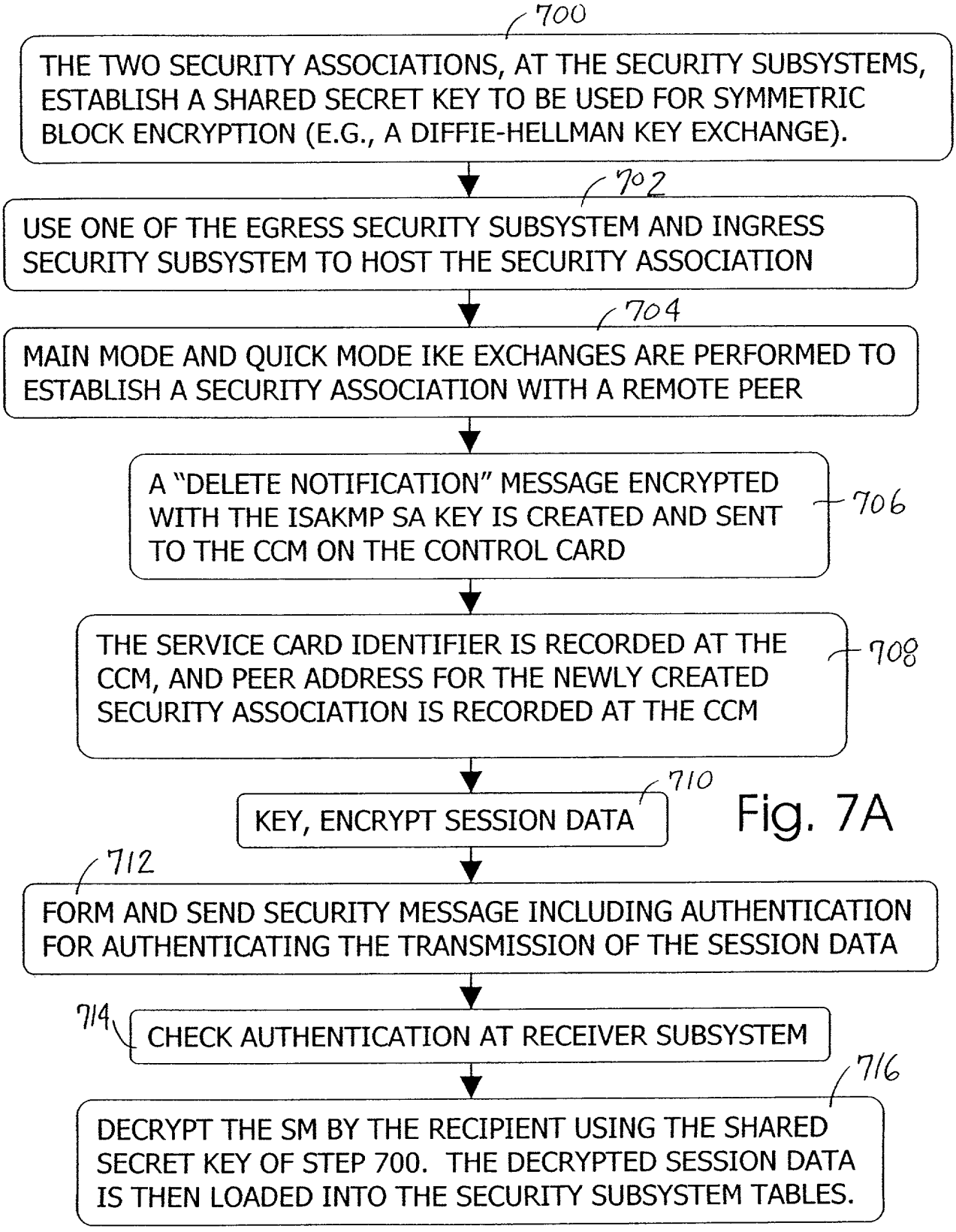
700
THE TWO SECURITY ASSOCIATIONS, AT THE SECURITY SUBSYSTEMS, ESTABLISH A SHARED SECRET KEY TO BE USED FOR SYMMETRIC BLOCK ENCRYPTION (E.G., A DIFFIE-HELLMAN KEY EXCHANGE).
702
USE ONE OF THE EGRESS SECURITY SUBSYSTEM AND INGRESS SECURITY SUBSYSTEM TO HOST THE SECURITY ASSOCIATION
704
MAIN MODE AND QUICK MODE IKE EXCHANGES ARE PERFORMED TO ESTABLISH A SECURITY ASSOCIATION WITH A REMOTE PEER
A "DELETE NOTIFICATION" MESSAGE ENCRYPTED WITH THE ISAKMP SA KEY IS CREATED AND SENT TO THE CCM ON THE CONTROL CARD
706
THE SERVICE CARD IDENTIFIER IS RECORDED AT THE CCM, AND PEER ADDRESS FOR THE NEWLY CREATED SECURITY ASSOCIATION IS RECORDED AT THE CCM
708
KEY, ENCRYPT SESSION DATA
710
712
FORM AND SEND SECURITY MESSAGE INCLUDING AUTHENTICATION FOR AUTHENTICATING THE TRANSMISSION OF THE SESSION DATA
714
CHECK AUTHENTICATION AT RECEIVER SUBSYSTEM
716
DECRYPT THE SM BY THE RECIPIENT USING THE SHARED SECRET KEY OF STEP 700. THE DECRYPTED SESSION DATA IS THEN LOADED INTO THE SECURITY SUBSYSTEM TABLES.

Fig. 7A

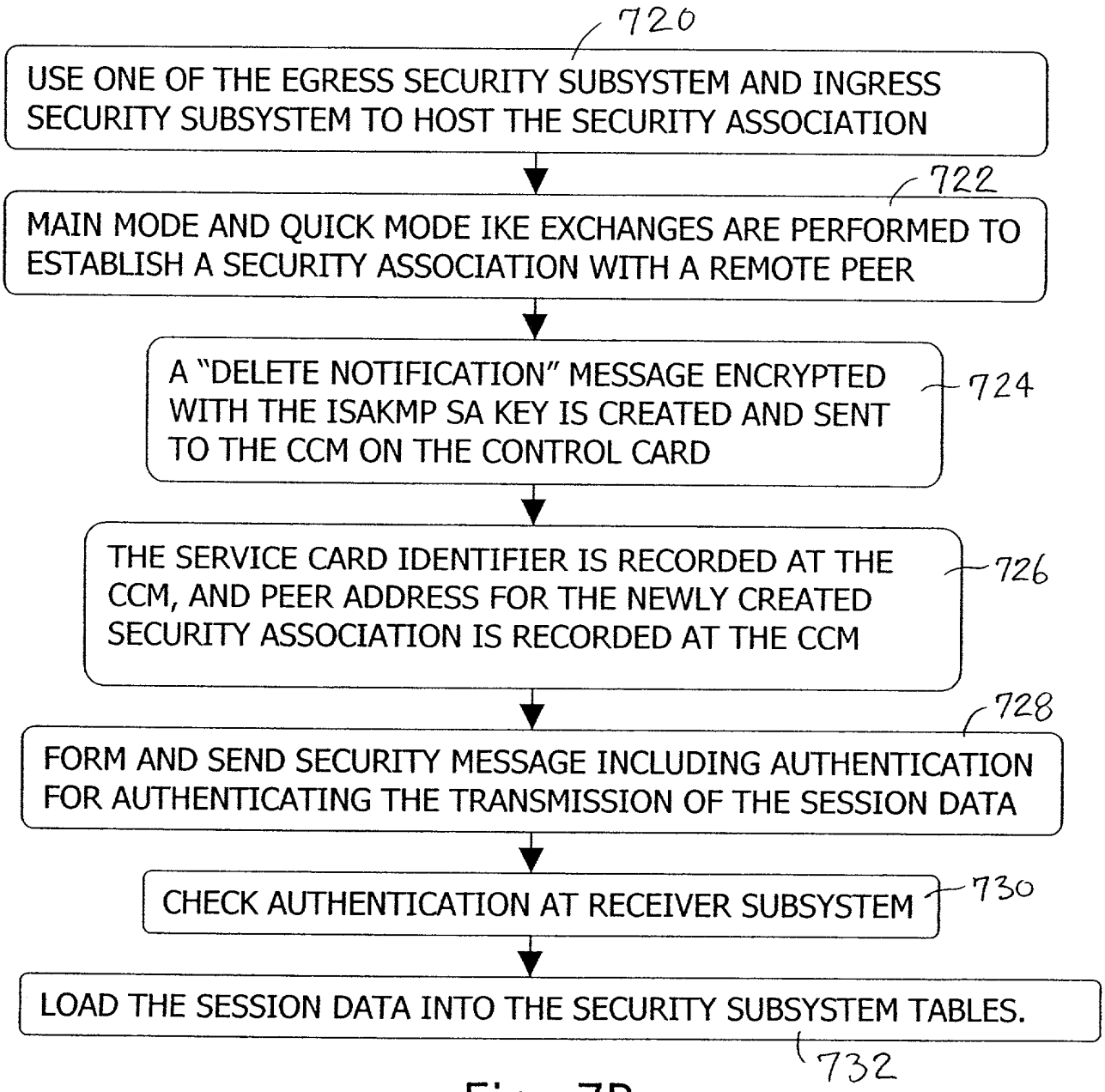
720
USE ONE OF THE EGRESS SECURITY SUBSYSTEM AND INGRESS SECURITY SUBSYSTEM TO HOST THE SECURITY ASSOCIATION
722
MAIN MODE AND QUICK MODE IKE EXCHANGES ARE PERFORMED TO ESTABLISH A SECURITY ASSOCIATION WITH A REMOTE PEER
A "DELETE NOTIFICATION" MESSAGE ENCRYPTED WITH THE ISAKMP SA KEY IS CREATED AND SENT TO THE CCM ON THE CONTROL CARD
724
THE SERVICE CARD IDENTIFIER IS RECORDED AT THE CCM, AND PEER ADDRESS FOR THE NEWLY CREATED SECURITY ASSOCIATION IS RECORDED AT THE CCM
726
728
FORM AND SEND SECURITY MESSAGE INCLUDING AUTHENTICATION FOR AUTHENTICATING THE TRANSMISSION OF THE SESSION DATA
CHECK AUTHENTICATION AT RECEIVER SUBSYSTEM
730
LOAD THE SESSION DATA INTO THE SECURITY SUBSYSTEM TABLES.
732

Fig. 7B

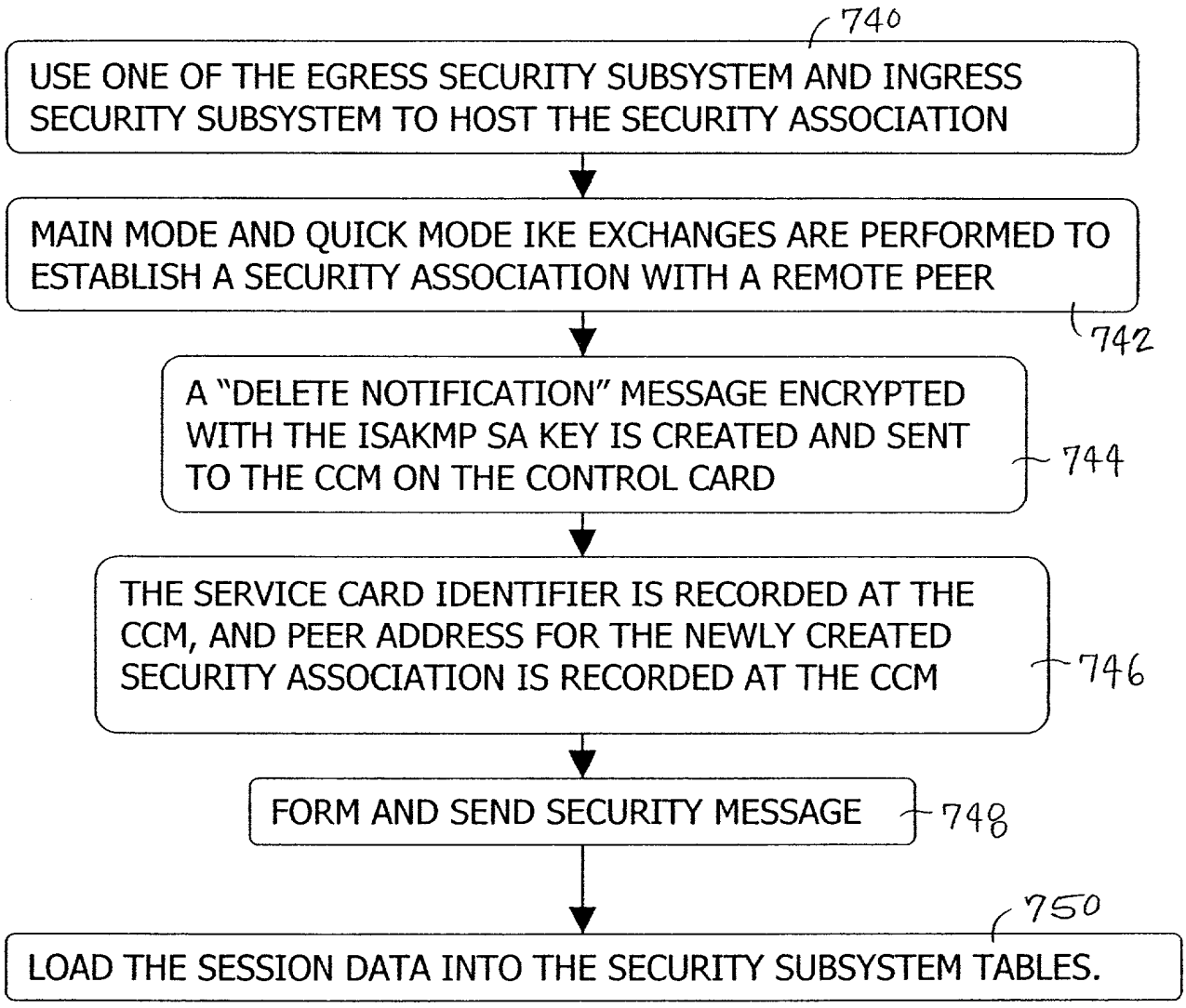
740
USE ONE OF THE EGRESS SECURITY SUBSYSTEM AND INGRESS SECURITY SUBSYSTEM TO HOST THE SECURITY ASSOCIATION
MAIN MODE AND QUICK MODE IKE EXCHANGES ARE PERFORMED TO ESTABLISH A SECURITY ASSOCIATION WITH A REMOTE PEER
742
A "DELETE NOTIFICATION" MESSAGE ENCRYPTED WITH THE ISAKMP SA KEY IS CREATED AND SENT TO THE CCM ON THE CONTROL CARD
744
THE SERVICE CARD IDENTIFIER IS RECORDED AT THE CCM, AND PEER ADDRESS FOR THE NEWLY CREATED SECURITY ASSOCIATION IS RECORDED AT THE CCM
746
FORM AND SEND SECURITY MESSAGE
748
750
LOAD THE SESSION DATA INTO THE SECURITY SUBSYSTEM TABLES.

Fig. 7C

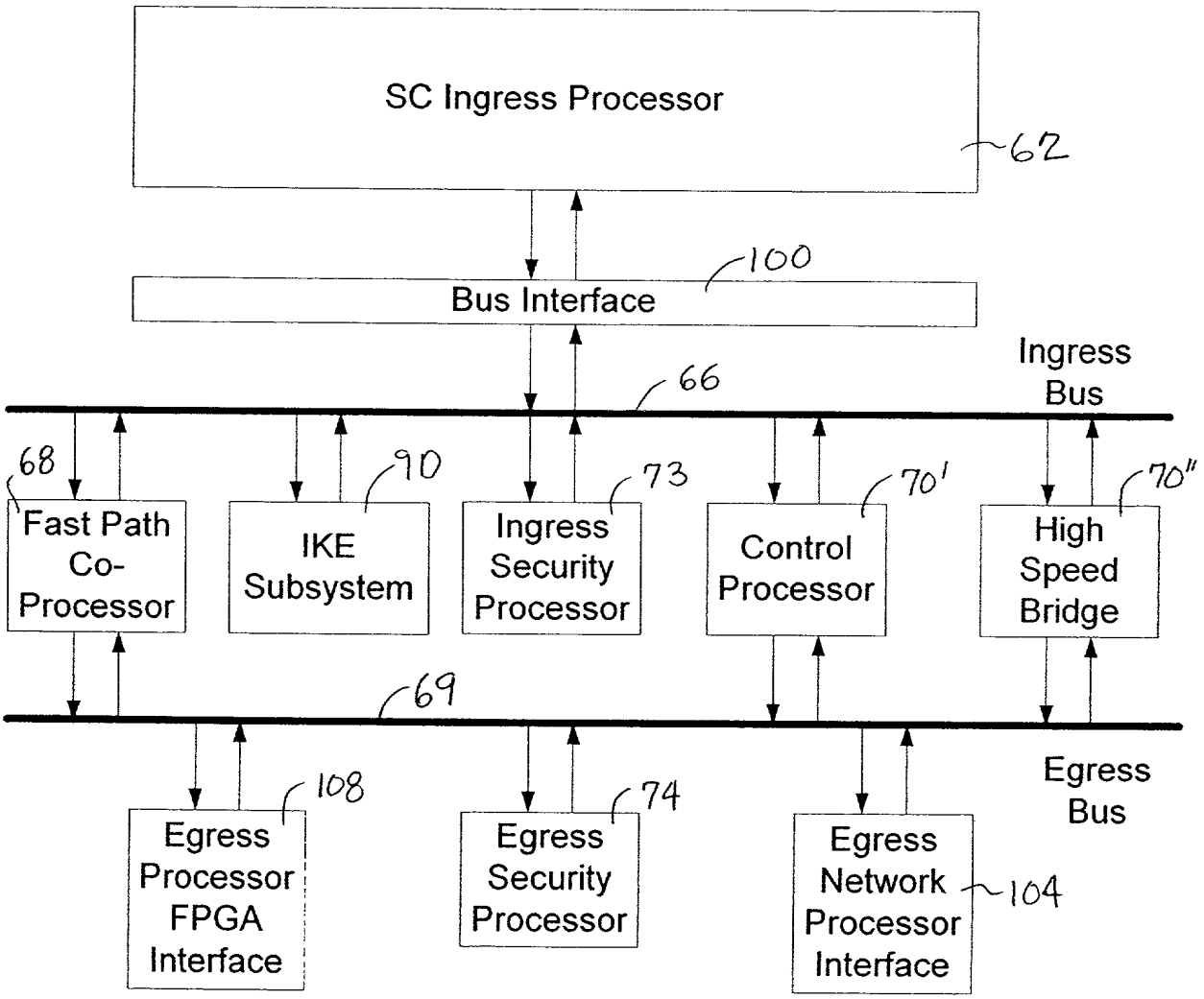
SC Ingress Processor
62
Bus Interface
100
Ingress Bus
66
68
Fast Path Co-Processor
IKE Subsystem
90
Ingress Security Processor
73
Control Processor
70'
High Speed Bridge
70"
69
Egress Bus
Egress Processor FPGA Interface
108
Egress Security Processor
74
Egress Network Processor Interface
104

Fig. 8